The Information Sharing Environment Privacy Guidelines
Executive Summary

In the post-9/11 world, sharing information to "connect the dots" in order to ensure the security of our nation continues to be a priority for the law enforcement, intelligence, defense, homeland security, and foreign affairs communities. As stated in the President's *National Strategy for Information Sharing* (October 2007):

> Our success in preventing future terrorist attacks depends on our ability to gather, analyze, and share information and intelligence regarding those who want to attack us, the tactics that they use, and the targets that they intend to attack.[1]

Integral to this sharing, which often includes sensitive personal information, is the protection of Americans' privacy, civil rights, and civil liberties. In addition to the U.S. Constitution, many laws and policies are already in place to protect these important rights, including the Privacy Act of 1974; the E-Government Act of 2002; and other federal laws, Executive Orders, and policies, as well as state, local, and tribal constitutions, laws, and policies.

The President, in implementing an Information Sharing Environment (ISE) that provides a conceptual framework and approach to facilitate the sharing of terrorism related information, has recognized the ongoing responsibility to protect Americans' privacy, civil rights, and civil liberties. To this end, he mandated the development and implementation of a set of privacy guidelines for the ISE (ISE Privacy Guidelines), the purpose of which is to maintain and build upon the privacy protections currently in place, while continuing to enhance the sharing of terrorism related information between agencies and at all levels of government, the private sector, and our foreign partners. Only by zealously protecting the privacy and other legal rights of Americans will confidence and support be maintained for these critical information sharing efforts.

Creation of the ISE

Since September 11, 2001, the nation's counterterrorism capabilities and the capacity to share information related to terrorism have improved significantly. Law enforcement and counterterrorism agencies have enhanced their ability to share information both horizontally and vertically and ensure the inclusion of public safety and private sector entities in information sharing efforts that are integral to preventing and ameliorating further acts of terrorism. Many processes have been created to improve information sharing, including overarching developments in creating and implementing the ISE.

The ISE was mandated by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) passed by Congress and signed by the President in December 2004. As defined by IRTPA, the ISE is "an approach that facilitates the sharing of terrorism-related information." Key to this definition is the understanding that the ISE is an approach, not

[1] *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (NSIS), October 2007, p. 1.

a place or a system. Its purpose is to enhance the sharing of terrorism related information[2] among and between federal, state, local, and tribal agencies and entities, the private sector, and our foreign partners in order to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism on the United States. Given the threat of terrorism, it is clearly time to address the impediments to information sharing for both classified and unclassified information, while, at the same time, protecting the information privacy and other legal rights of Americans.

Function of the ISE

The ISE is the sum of the policies, processes, protocols, and technologies that enable the sharing of terrorism-related information among the ISE community. It brings together, aligns, and builds upon existing information policies, business processes, and technologies by promoting a culture of information sharing through increased collaboration.[3] Core to the success of the ISE is the achievement of greater information sharing by facilitating, rather than hindering, the sharing of terrorism related information among those who need it.

The ISE has four priority areas:

- Improving Sharing Practices—by standardizing ISE management practices in trusted partnerships through validating and standardizing ISE policies, business processes, and technologies through operational activities.
- Creating a Culture of Sharing—by providing privacy protection, performance management, and training.
- Reducing Barriers—by building common standards for acquiring, sharing, and using ISE information.
- Institutionalizing Sharing—by setting common legal, policy guidance, architecture, and standards; improving business processes; and leveraging resources, progress, and systems that meet ISE core elements.

Program Manager for the Information Sharing Environment and the Information Sharing Council

To manage the implementation of the ISE, IRTPA required the President to designate a Program Manager to:

> Manage the ISE, oversee its implementation, assist in the development of ISE standards and practices, and monitor and assess its implementation by Federal departments and agencies. The law also established an Information Sharing Council to advise the President and the Program Manager on the development of ISE policies, procedures, guidelines, and standards, and to ensure proper coordination among federal departments and agencies participating in the ISE.

[2] Terrorism related information means terrorism information, including information on weapons of mass destruction, homeland security information, and law enforcement information related to terrorism.
[3] Program Manager, Information Sharing Environment Web site, "*About the ISE, What Is in the ISE?*" http://www.ise.gov/content/about.htm#faqAnchor_1.

> Accordingly, the President designated the Program Manager and directed that the Program Manager and his staff be located in the Office of the Director of National Intelligence. On October 25, 2005, the President issued Executive Order 13388, superseding Executive Order 13356, to facilitate the work of the Program Manager, expedite the establishment of the ISE, and restructure the Information Sharing Council [ISC].[4]

The ISC actively consults with representatives from other Federal departments and agencies as well as the U.S. Department of Justice's Global Justice Information Sharing Initiative; state, local, and tribal partners; and key private sector groups.[5] This coordination ensures that all applicable entities understand the ISE, have input in its implementation, and take a proactive role regarding its execution within their agencies and organizations.

ISE Privacy Guidelines

As noted, one of the biggest challenges in sharing terrorism related information is balancing national security needs with protecting the privacy and civil liberties of individuals.

> On December 16, 2005, in accordance with section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, the President issued a Memorandum to Heads of Executive Departments and Agencies prescribing the guidelines and requirements in support of the creation and implementation of the ISE.[6]

In Guideline 5 of this Memorandum:

> The President directed, as he did earlier in Executive Order 13353, that the information privacy rights and other legal rights of Americans must be protected. Accordingly, he required guidelines be developed and submitted for approval to ensure such rights are protected in the implementation and operation of the ISE.[7]

[4] NSIS, p. 12.
[5] McNamara, Ambassador Thomas, "*Statement for the Record to the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Part IV, A Presidential Priority*," p. 4, April 26, 2007, http://www.ise.gov/docs/HHSC-20070426-%20McNamara%20Testimony.pdf.
[6] NSIS, p. 12.
[7] NSIS, p. 13.

In December 2006, the President approved for issuance by the Program Manager the *Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment* (ISE Privacy Guidelines or Guidelines). The ISE Privacy Guidelines apply to federal departments and agencies regarding information about U.S. citizens and lawful permanent residents (protected information) that is subject to information privacy and other legal protections under the U.S. Constitution and federal laws of the United States. Nonfederal entities seeking access to federal agency data will need to ensure that they develop and implement appropriate policies that provide privacy protections that are *at least as comprehensive* as the ISE Privacy Guidelines.

The ISE Privacy Guidelines provide a privacy protection framework that requires agencies to implement core privacy protections, such as data quality, redress, and data security, for ISE information. Additionally, the Guidelines establish principles that require specific uniform action across the ISE that reflects basic privacy protections and best practices. They require each agency participating in the ISE to put in place adequate processes and procedures designated to protect privacy and civil liberties based on the rules and mission of the agency. The Guidelines create a government-wide process for ensuring that privacy and other legal protections are raised and addressed in a consistent manner throughout the ISE development process by each agency.

> Successful implementation of the Privacy Guidelines requires a governance structure to monitor compliance and to revise the Guidelines as we gain more experience. The President, therefore, directed the Program Manager to establish the ISE Privacy Guidelines Committee. The Committee is chaired by representatives of the Attorney General and the Director of National Intelligence, and consists of the Privacy Officials of the departments and agencies of the Information Sharing Council. The Committee seeks to ensure consistency and standardization, as well as serve as a forum to share best practices and resolve agency concerns.[8]

The Guidelines suggest a three-step privacy protection methodology for the ISE that has been recommended by the ISE Privacy Guidelines Committee (PGC)—identify, assess, and protect. The first step is to *identify* laws, Executive Orders, policies, and procedures that address privacy and other legal protections as well as the systems, sharing arrangements, and protected information that are or may be shared in the ISE. Second is to *assess* laws, policies, systems, and sharing arrangements to determine whether they meet the core protections required by the ISE Privacy Guidelines. Third is to *protect* the privacy and civil liberties of Americans by applying the core ISE Privacy Guidelines provisions to the systems and sharing arrangements. To assist agencies in implementing the ISE Privacy Guidelines, the PGC has developed an Implementation Manual to provide guidance and resources when applying the Guidelines to the agency's information sharing arrangements.

[8] NSIS, p. 28.

ISE Privacy Guidelines Implementation Manual

The ISE Privacy Guidelines implementation manual[9] offers federal agencies assistance and guidance in implementing the ISE Privacy Guidelines. Formulating and implementing the policies, procedures, and practices required by the ISE Privacy Guidelines is mandatory. However, recognizing the many different environments in which the ISE Privacy Guidelines must be implemented, the manual is designed to accommodate agency-specific organizational structures, practices, and authorities. The tools and practices reflected in the manual are not prescriptive but are offered as suggestions, to be used as appropriate by ISE participants.

The manual is designed to provide "one-stop shopping" for information, resources, tools, and guidance on the ISE Privacy Guidelines. The manual supports agencies in understanding and implementing the ISE Privacy Guidelines while minimizing duplication of effort and ensuring consistent interpretation of the Guidelines. It provides agencies with a "how to" on implementing the ISE Privacy Guidelines, cites applicable authorities, details the PGC governance structure, clarifies Guidelines requirements, and provides resources, tools, and best practices and lessons learned from implementation activities. It does not impose new policy requirements on agencies.

Implementing the ISE Privacy Guidelines is an ongoing challenge. There exists no proven formula for reconciling and balancing national security and privacy, an issue that our nation has confronted since its founding. The ISE Privacy Guidelines manual will assist agencies to carry out their responsibilities to share terrorism-related information in accordance with ISE requirements while protecting the information privacy and other legal rights of Americans, a key to the success of the ISE.

[9] The ISE Privacy Guidelines Implementation Manual can be accessed on the ISE Web site at www.ise.gov.